

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
3 May 2001 (03.05.2001)

PCT

(10) International Publication Number
WO 01/31822 A1

(51) International Patent Classification⁷: **H04J 3/24,**
H04L 12/46, G06F 15/16

Apt. 103, Parsippany, NJ 07054 (US). **MCAULEY, Anthony;** 150 Linden Avenue, Glen Ridge, NJ 07028 (US). **SHOBATAKE, Yasuro;** 331 Newman Springs Road, Red Bank, NJ 07701 (US).

(21) International Application Number: **PCT/US00/29055**

(22) International Filing Date: 20 October 2000 (20.10.2000)

(74) Agents: **COCKINGS, Orville et al.;** c/o International Coordinator, Telcordia Technologies, Inc., 445 South Street, Rm. 1G112R, Morristown, NJ 07960-6438 (US).

(25) Filing Language: English

(81) Designated States (*national*): CA, JP.

(26) Publication Language: English

(84) Designated States (*regional*): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

(30) Priority Data:
60/161,220 22 October 1999 (22.10.1999) US

Published:

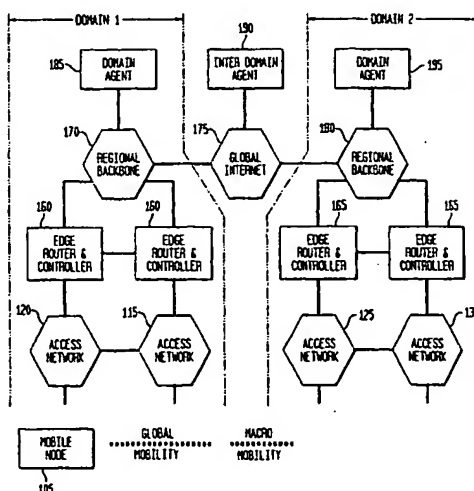
- With international search report.
- Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.

(71) Applicants: **TELCORDIA TECHNOLOGIES, INC.** [US/US]; 445 South Street, Morristown, NJ 07960-6438 (US). **TOSHIBA AMERICA RESEARCH, INC.** [US/US]; P.O. Box 136, Convent Station, NJ 07961-0136 (US).

(72) Inventors: **BABA, Shinichi;** 12 Pilgrim Court, Morristown, NJ 07960 (US). **DAS, Subir;** 350 Parsippany Road,

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR DYNAMIC REGISTRATION AND CONFIGURATION PROTOCOL



(57) Abstract: The Dynamic Registration and Configuration Protocol (DRCP) provides a framework for registering and passing configuration information to roaming mobile hosts (105). DRCP is compatible with DHCP and can switch to using DHCP protocol if only DHCP servers (165) are present in the network (175). Most importantly, DRCP allows rapid configuration by moving address consistency checking from the critical path. Other novel features of DRCP allow: a) clients to know when to get a new address independent of the layer-2 access technology, b) efficient use of scarce wireless bandwidth, c) clients to be routers, d) dynamic addition or deletion of address pools to any DRCP node, and e) message exchange without broadcast.



WO 01/31822 A1

BEST AVAILABLE COPY

METHOD AND SYSTEM FOR DYNAMIC REGISTRATION AND CONFIGURATION PROTOCOL

RELATED UNITED STATES APPLICATIONS/CLAIM OF PRIORITY

5 This patent application is a non-provisional counterpart to, and claims the benefit of priority of provisional application serial number 60/161,220, which was filed on October 22, 1999.

TECHNICAL FIELD OF THE INVENTION

10 The present invention relates generally to networks and more specifically to a method, system, apparatus and product for providing dynamic registration and configuration of mobile clients in end to end wireless/wireline Internet Protocol (IP) networks.

15 BACKGROUND

 Various TCP/IP registration and configuration network protocols exist today. Popular protocols include: Mobile IP (MIP) and Dynamic Host Configuration Protocol (DHCP). Although its primary function is providing location services and continuous connectivity to roaming users, Mobile IP also provides for flexible registration and
20 configuration capabilities. The Mobile IP client sends registration information to a Foreign Agent on the Layer 2 network to which the client is connected. The Foreign Agent can then configure the client, after getting authorization from the user's Home Agent. While Mobile IP is a solution to manage device mobility throughout the global Internet, its costs can be too high for many applications, and it is not compatible with
25 the widely deployed DHCP.

For example, Mobile IP provides networks transparency above the IP layer. This transparency is achieved at a relatively high cost (e.g., triangular routing) compared to simply getting a new care-of-address. In many cases, however, this transparency is not needed, e.g., for web browsing.

5

The Dynamic Host Configuration Protocol (DHCP) provides a well-tested and widely-deployed framework for passing configuration information to network hosts. By means of dynamic allocation of IP addresses, DHCP allows for leasing of network addresses, recovery of network addresses upon expiration of those leases, as well as
10 subsequent re-use or reallocation of network addresses. DHCP, however, was designed for hosts on a fixed LAN, not for mobile hosts roaming among commercial wireless networks.

Rapid configuration (milliseconds rather than seconds) is necessary for most
15 roaming users. DHCP specification says a client should, and most implementations do, the widely known Address Re-use Protocol (ARP) check after it receives an assigned address before the assigned address is used by the client. This checking by the client typically results in a long delay before communication can resume.

20 Other limitations of DHCP are that it: (a) has no facilities for detecting a move to a new subnet, (b) involves a large message size (parts of which are not needed), (c) requires a DHCP node to be a server or a relay agent, and not both, and (d) identifies machines (e.g., by MAC address) rather than users (e.g., by a network access identifier of the form such as user@domain). The fixed functionality limits architectural choices
25 that might be attractive to wireless service providers, where a subnet router may act as a

relay agent when a node first moves into the domain, but as a server for previously authorized nodes.

Given the foregoing, there is a need for a solution which can address the
5 problems of the prior art and provide for rapid client registration and configuration of a
roaming mobile host. The registration functionality would enable roaming mobile hosts
to rapidly and automatically register their presence and their requirements with
networks. The configuration functionality would enable networks to automatically
configure roaming mobile hosts to the particular network characteristics. Moreover,
10 there is a need for a solution which provides efficient use of scarce wireless bandwidth,
allows mobile hosts to be routers, allows flexible proxies that can act as both relay or
server and allows dynamic server and relay reconfiguration.

SUMMARY

15 The present invention, hereinafter referred to as the Dynamic Registration and
Configuration Protocol (DRCP) is a protocol directed to solving the foregoing needs. In
a basic application, DRCP, although providing some new configuration capability, has
no other function except registration and configuration. In more advanced applications,
DRCP provides additional functionality, including providing information about the
20 location of a network registration, service negotiation, or mobility agent.

DRCP is built directly on UDP and IP and is a lightweight dynamic
configuration protocol. DRCP provides the critical functions necessary for roaming
users. For example, DRCP allows rapid configuration by moving address
25 consistency checking from the critical path. Other features and/or advantages allow:

a) clients to know when to get a new address independent of the layer-2 access technology, b) efficient use of scarce wireless bandwidth, c) clients to be routers, d) dynamic addition or deletion of address pools to any DRCP node, and e) message exchange without broadcast.

5

Therefore, in accordance with one aspect of the present invention, there is provided, a system, method, apparatus and product for rapidly and dynamically registering and configuring a mobile client in a second network environment; said mobile client having traveled from a first network environment to said second network environment, said method comprising:

10 providing a plurality of valid IP addresses associated with said second network environment for assignment to mobile clients; said valid IP addresses having been positively checked for availability; broadcasting a request for at least one of said plurality of valid IP addresses;

15 monitoring said first network environment to sense movement of said mobile client from said first Network environment to said second network environment to provide a request for a valid IP address; and providing at least one of said plurality of valid IP addresses associated with said second network environment to be assigned to said mobile client.

20

In accordance with a second aspect of the present invention, there is provided a data structure representing a signaling message having a small footprint to provide efficient use of scarce wireless bandwidth,

25

These and other aspects, features and advantages of the present invention will

become better understood with regard to the following description, appended claims, and accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWING(S)

5 Turning now to the drawings:

Figure 1 is a high level functional architecture of an IP-based network having mobile nodes in communication with various wired or wireless access networks.

10 Figure 2 is an embodiment of a DRCP client-server model in accordance with the teachings of the present invention.

Figure 3 is one embodiment of a DRCP client message format in accordance with the teachings of the present invention.

15

Figure 4 is one embodiment of a DRCP server message format in accordance with the teachings of the present invention.

Figure 5 is one embodiment of an OPCODE field of a DRCP message in
20 accordance with the teachings of the present invention.

Figure 6 is one embodiment of an OPTION field of a DRCP message in accordance with the teachings of the present invention.

25 Figure 7 illustrates a preferred DRCP signaling and message flow sequence

when a DRCP client moves into a new administrative domain and/or subnet.

Figure 8 illustrates a preferred DRCP signaling and message flow sequence when a DRCP extending a lease within an administrative domain.

5

Figure 9 illustrates a preferred DRCP signaling and message flow sequence when a DRCP client re-negotiating an OFFER message sent by a DRCP server.

10 **DETAILED DESCRIPTION OF THE PRESENT INVENTION**

Referring more specifically to the drawings, for illustrative purposes the present invention is embodied in the system configuration, method of operation and product or computer-readable medium such as floppy disks, conventional hard disks, CD-ROMS, Flash ROMS, nonvolatile ROM, RAM and any other equivalent computer memory device, generally shown in Figures 1 – 9. It will be appreciated that the system, method of operation and product may vary as to the details of its configuration and operation without departing from the basic concepts as disclosed herein.

15

ARCHITECTURE

20

Figure 1 is a high level network architecture diagram of an IP based network that is suitable for implementing DRCP. As shown,, the network comprises a plurality of components in communication with each other; the components comprising: at least one mobile client 105, access networks 115-130, edge routers and controllers 160, 165, regional backbones 170, 180, domain agents 185, 195, an inter domain agent 190 and

25

the global Internet 175. Each of the forgoing components are well-known in the art and accordingly will not be discussed. Figure 1 is meant to be very general functional diagram. It does not, for example, specify where a base station is located. A base station could be located within the access networks, thus being a Layer 2 base station or located within the edge router, thus being an IP base station. Moreover, the Domain and Inter-Domain agents, which perform functions such as registration and AAA, are shown as separate single boxes; however each could be implemented as multiple nodes (possibly in a hierarchical structure).

10 DRCP is based on a client-server model. Figure 2 shows how the DRCP client and DRCP server may map onto the architecture shown in Figure 1. The DRCP client-server model is similar to the DHCP client-server in most respects. There are, however, some differences.

15 First, unlike DHCP, any DRCP node (including the client) can be on a router or host. Second, unlike DHCP, all DRCP nodes run the same program. The only thing that makes a DRCP node a server is that it has configuration information, including an address pool and other configuration parameters to be used on an interface. A DRCP server must configure its own interface using the configuration
20 information for that subnet. This allows for more flexible and robust operation.

DRCP MESSAGE FORMATS

DRCP messages have the same basic semantics as those used in DHCP. For example, a DHCPOFFER message has the same basic functions (and

name) as a DRCP_OFFER message. New DRCP messages are needed, however, in order to minimize message size thereby providing use of scarce wireless bandwidth.

Like DHCP, DRCP uses UDP as its transport protocol. All DRCP messages are sent in UDP/IP packets to special DRCP ports and, are preferably, 32-bit aligned. There

5 are two types of DRCP signaling messages running on three different DRCP ports:

a) All messages from a DRCP client are sent to the DRCP_SERVER_PORT port.

b) All messages from a DRCP server are sent to the DRCP_CLIENT_PORT port,
10 except the DRCP_ADVERTISEMENT.

c) DRCP_ADVERTISEMENT messages from a DRCP server are sent to the DRCP_ADVERTISEMENT_PORT port on the DRCP client.

15 What follows is a list and description of typical DRCP client messages sent by a DRCP client.

DRCP_DISCOVER: Registration message sent by a DRCP-client on its local subnet to request a new address and other configuration parameters. While a
20 DHCPDISCOVER message must be broadcast [DHC], a DRCP_DISCOVER message may be broadcast or unicast depending whether the client knows the address of a DRCP Server (e.g., from a DRCP_ADVERTISEMENT).

DRCP_REQUEST: Registration message sent by a DRCP-client on its local subnet to
25 request extending the lease on an address.

DRCP_INFORM: Registration message sent by a DRCP-client on its local subnet to request new configuration parameters. This could be used, for example, if the client already has an externally configured network address.

5

DRCP_DECLINE: Registration message sent by a DRCP-client on its local subnet to request a different address, either because the one assigned is not acceptable (e.g., it is already in use by another client) or because the client has moved to a new subnet.

10

DRCP_RELEASE: De-registration message sent by a DRCP-client on its local subnet to relinquish a network address and cancel remaining lease.

DRCP_ACCEPT: Registration message sent by a DRCP-client on its local subnet in response to an OFFER from servers. The client accepts offered parameters from one server and implicitly declining offers from all others.

15

What follows is a list and description of typical DRCP server messages sent by a DRCP server.

20

DRCP_OFFER: Configuration message sent back to client on the same subnet where the DRCP server node received a DRCP_DISCOVER message.

DRCP_ACK: Configuration message broadcast by a Server on its local subnet in response to a DRCP_ACCEPT.

25

DRCP_NAK: Message sent to a client or clients (may be broadcast) to tell them not to use an address or other service they requested. (e.g., when a client is using a wrong address).

5

DRCP_ADVERTISEMENT: Server periodically broadcasts (or unicast in response to a client using an incorrect address) the network information (such as Server IP address or Network address). Listening to this, client can understand the subnet change.

10

All DRCP messages from the DRCP client (to the DRCP_SERVER_PORT) have the same general format (size shown in braces) as shown in Figure 3: The various fields are:

| | | | |
|----|--------------|---------------|--|
| 15 | <u>FIELD</u> | <u>OCTETS</u> | <u>DESCRIPTION</u> |
| | op | 1 | Message OpCode. |
| | htype | 1 | Hardware address type. |
| | hlen | 1 | Hardware address length in bytes. |
| | xid | 1 | Transaction ID. |
| 20 | chaddr | var. | Client hardware address (e.g 16 bytes for 802.X) |
| | options | var. | Optional parameters field. |

All DRCP server messages from the DRCP server (to the DRCP_CLIENT_PORT) have the same general format (except a DRCP_ADVERTISEMENT) as shown in Figure 4. The fields are the same as those of the DRCP client message format except that it includes an additional field: ciaddr.

5

| FIELD | OCTETS | DESCRIPTION |
|--------|--------|-------------------|
| ----- | ----- | ----- |
| ciaddr | 4 | Client IP address |

10 What follows is a description of the content of the various field shown in Figures 3 and 4:

The opcode field consists of version number (ver), message type (mtype) and broadcast(B) flag as shown in Figure 5.

15

Possible values for Message types include:

| | Message Value | Message Type |
|----|---------------|---------------|
| | ----- | ----- |
| 20 | 0 0 0 1 | DRCP_DISCOVER |
| | 0 0 1 0 | DRCP_REQUEST |
| | 0 0 1 1 | DRCP_INFORM |
| | 0 1 0 0 | DRCP_ACCEPT |
| | 0 1 0 1 | DRCP_DECLINE |
| 25 | 0 1 1 1 | DRCP_RELEASE |

| | |
|---------|--------------------|
| 1 0 0 1 | DRCP_OFFER |
| 1 0 1 0 | DRCP_ACK |
| 1 0 1 1 | DRCP_NAK |
| 1 1 1 1 | DRCP_ADVERTISEMENT |

5

Htype: see ARP section in "Assigned Numbers" RFC. For example: Htype = '1' means it is a 10mb ethernet.

10 Hlen: Length of chaddr field in bytes. For example Hlen is set to '6' for 10mbps ethernet.

Xid: A random number chosen by the client. It is used by the client and server to associate messages and responses between a client and a server.

15

Ciaddr: The IP address assigned to a client by a server.

Options: All information, other than what is in the common header, must be included as options. All options have a common 4 byte header as shown in Figure 6.

20

METHOD OF OPERATION

A node is initially assumed to only know its interfaces which are running the DRCP-client and its security associations. If there are multiple interfaces, each interface may be configured in a different way. For example, one interface may be
25 configured by DRCP, another using a locally stored address, and a third as a DHCP-

client. After boot-up, however, any interface configured as a DRCP interface listens to messages on a specified port designated a DRCP_ADVERTISEMENT_PORT. During any message exchange a transaction id is used between the client and server and they must match for a given exchange.

5

If a DRCP interface does not have a local address pool it becomes a DRCP client. The client first broadcasts a DRCP_DISCOVER message (similar to a DHCPDISCOVER message) to a designated port on the DRCP server, i.e. DRCP_SERVER_PORT. It then listens for a response. If it gets no response after a
10 predetermined time-out period, i.e., DRCP_RETX_TIMEOUT, it resends the DISCOVER message. This process repeats for up to a predetermined number of retransmissions, i.e. DRCP_RETX_MAX.

If an unconfigured DRCP client receives a DRCP_ADVERTISEMENT
15 message (on the DRCP_ADVERTISEMENT_PORT), then it will change to a unicast state, so the next DRCP_DISCOVER message will be unicast to the source address of the DRCP_ADVERTISEMENT message.

If the DRCP client receives an OFFER message, it can immediately configure
20 its interface with that address. There is no requirement to do ARP checking (as in DHCP). After getting an address the DRCP client may periodically send out DRCP_REQUEST messages to renew the lease. These message are retransmitted until acknowledged by a DHCP_ACK message.

If a configured DRCP client receives a DRCP_ADVERTISEMENT message (on the DRCP_ADVERTISEMENT_PORT), then it will check if it can still use the same IP address. If it cannot use the same IP address, then the client must unicast a new DRCP_DISCOVER message in order to get a new address. This helps to detect the subnet change. It happens only when a client moves to a new subnet.

If a DRCP interface has a local configuration information (including an address pool) for that interface, then it becomes a DRCP server. The DRCP server must first use the first address from the address pool to configure its own interface. It can then use the rest of the address pool to allocate individual addresses directly to DRCP clients on the same subnet as that interface.

The DRCP server may send periodic DRCP_ADVERTISEMENT messages (on the DRCP_ADVERTISEMENT_PORT) every DRCP_ADVERTISEMENT_PERIOD time.

The server listens for a DHCP_DISCOVER broadcast or unicast message on its designated port, i.e., DRCP_SERVER_PORT. If it gets a DHCP_DISCOVER message, then the DRCP server can immediately send a DRCP_OFFER message with valid IP address and other configuration parameters from its configuration information. The DRCP_OFFER message will be resent for a predetermined time period, every DRCP_OFFER_PERIOD for up to DRCP_SERVER_MAX retransmissions, or until it receives a DRCP_ACCEPT or DRCP_DECLINE message from a DRCP client.

Figure 7 depicts the signaling and message flow when a DRCP client moves into a new administrative domain and/or subnet. At 701, the DRCP server initiates periodic ADVERTISEMENT messages. Upon receiving the ADVERTISEMENT message, at 702, the DRCP client transmits and retransmits the DISCOVER message until it gets an OFFER message or the timer expires. At 703, the DRCP server transmits and retransmits the OFFER message until it gets an ACCEPT or DECLINE message, at 704, or the timer expires. Notably, a key difference between DRCP and DHCP is that there is no ACK message from the DRCP server to the DRCP client. Also, a DRCP client accepts with an ACCEPT rather than a REQUEST message. A second key difference is that configuration can be used as soon as the OFFER message is received by the DRCP client (duplicate detection is handled in the background).

Figure 8 depicts the signaling and message flow when a DRCP client renews or releases an existing lease. If a DRCP client wants to renew or release its lease, then there will be a flow of DRCP messages as follows: At 801, a DRCP client sends a message requesting a renewal or a release of an existing lease. At 802, a DRCP server sends an ACK message in response to the REQUEST/RELEASE message.

Figure 9 depicts the signaling and message flow when a DRCP client renegotiates its OFFER message. At 901, a DRCP client sends an OFFER message to a DRCP client. At 902, the DRCP client sends a DECLINE message to the DRCP server. At 903, upon receiving the DECLINE message the DRCP server can either do nothing or it can send a new OFFER message to the DRCP client. At 903, in response to the new OFFER message, the DRCP client can either decline the OFFER

message again and send another DECLINE message or it can accept the OFFER message and send an ACCEPT message to the DRCP server.

Having now described a preferred embodiment of the invention, it should be
5 apparent to those skilled in the art that the foregoing is illustrative only and not
limiting, having been presented by way of example only. All the features disclosed in
this specification (including any accompanying claims, abstract, and drawings) may be
replaced by alternative features serving the same purpose, and equivalents or similar
purpose, unless expressly stated otherwise. Therefore, numerous other embodiments of
10 the modifications thereof are contemplated as falling within the scope of the present
invention as defined by the appended claims and equivalents thereto.

CLAIMS

What is claimed is:

- 5 1. A method for rapidly and dynamically registering and configuring a mobile client in a second network environment; said mobile client having traveled from a first network environment to said second network environment, said method comprising:
providing a plurality of valid IP addresses associated with said second network environment for assignment to mobile clients; said valid IP addresses having been
10 positively checked for availability;
broadcasting a request for at least one of said plurality of valid IP addresses;
monitoring said first network environment to sense movement of said mobile client from said first Network environment to said second network environment to provide a request for a valid IP address; and
15 providing at least one of said plurality of valid IP addresses associated with said second network environment to be assigned to said mobile client.
2. A computer-readable medium having computer-executable instructions for performing a method for rapidly and dynamically registering and configuring a mobile
20 client in a second network environment; said mobile client having traveled from a first network environment to said second network environment, comprising:
providing a plurality of valid IP addresses associated with said second network environment for assignment to mobile clients; said valid IP addresses having been positively checked for availability;
25 broadcasting a request for at least one of said plurality of valid IP addresses;

monitoring said first network environment to sense movement of said mobile client
from said first Network environment to said second network environment to provide a
request for a valid IP address; and
providing at least one of said plurality of valid IP addresses associated with said
5 second network environment to be assigned to said mobile client.

3. A system for rapidly and dynamically registering and configuring a mobile client in
a second network environment; said mobile client having traveled from a first network
environment to said second network environment, comprising:
10 at least one processor programmed to:
provide a plurality of valid IP addresses associated with said second network
environment for assignment to mobile clients; said valid IP addresses having
been positively checked for availability;
broadcast a request for at least one of said plurality of valid IP addresses;
15 monitor said first network environment to sense movement of said mobile client
from said first Network environment to said second network environment to
provide a request for a valid IP address; and
provide at least one of said plurality of valid IP addresses associated with said
second network environment to be assigned to said mobile client.

20

4. A computer-readable medium having stored thereon a data structure representing a
signaling message having a small footprint to be sent from a mobile client to a server,
said data structure comprising:
a first field containing data representing a message opcode;
25 a second field containing data representing a hardware address type;

a third field containing data representing a hardware address length;
a fourth field containing data representing a transaction ID;
a fifth field containing data representing a hardware address of said mobile client.

5 5. A data structure as in claim 4 further comprising a sixth field containing data representing one or more optional parameters.

6. A data structure as in claim 4 wherein said data representing said message opcode includes data representing a version number, a message type and a broadcast flag.

10

7. A data structure as in claim 6 wherein said message type is chosen from the group consisting of a DISCOVER, REQUEST, INFORM, ACCEPT, DECLINE, RELEASE, OFFER, ACK, NAK ADVERTISEMENT message type.

15 8. A computer-readable medium having stored thereon a data structure representing a signaling message having a small footprint to be sent by a server to a mobile mobile client, said data structure comprising:

a first field containing data representing a message opcode;

a second field containing data representing a hardware address type;

20 a third field containing data representing a hardware address length;

a fourth field containing data representing a transaction ID;

a fifth field containing data representing a hardware address of said mobile client; and

a sixth field containing data representing an IP address of said mobile client.

25

9. A data structure as in claim 8 further comprising a seventh field containing data representing one or more optional parameters;

10. A data structure as in claim 8 wherein said data representing said message opcode
5 includes data representing a version number, a message type and a broadcast flag.

11. A data structure as in claim 10 wherein said message type is chosen from the group consisting of a DISCOVER, REQUEST, INFORM, ACCEPT, DECLINE, RELEASE, OFFER, ACK, NAK ADVERTISEMENT message type.

10

12. In an IP based network, a method for rapidly and dynamically registering and configuring a mobile client in a second network environment; said mobile client having traveled from a first network environment to said second network environment, said method comprising:

15 providing at least one server in communication with said IP based network, said server having a pool of IP addresses and configuration parameters;
said server:

performing ARP checking on said IP address pool to provide a pool of valid IP addresses;

20 listening for a request for an IP address from a mobile client;

offering a valid IP address; and

sending said valid IP address and said configuration parameters to said mobile client thereby eliminating the need for said mobile client to itself perform ARP checking of said valid IP address.

25

13. A method as in claim 12 further comprising said server repeatedly offering said valid IP address until either a predetermined time period has expired, a predetermined number of offer transmissions has expired or a mobile client has responded to said offer of an IP address.

5

14. In an IP based network, an apparatus for rapidly and dynamically registering and configuring a mobile client in a second network environment; said mobile client having traveled from a first network environment to said second network environment; said apparatus comprising:

10 at least one server having an interface for communicating within said IP based network, said server having configuration parameters and a pool of IP addresses; said server programmed to:

perform ARP checking on said IP address pool to provide a pool of valid IP addresses;

15 listen for a request for an IP address from a mobile client; offer a valid IP address; and send said valid IP address and said configuration parameters to said mobile client thereby eliminating the need for said mobile client to itself perform ARP checking of said valid IP address.

20

15. An apparatus as in claim 14 wherein said server is further programmed to repeatedly offer said valid IP address until either a predetermined time period has expired, a predetermined number of offer transmissions has expired or a mobile client has responded to said offer of an IP address.

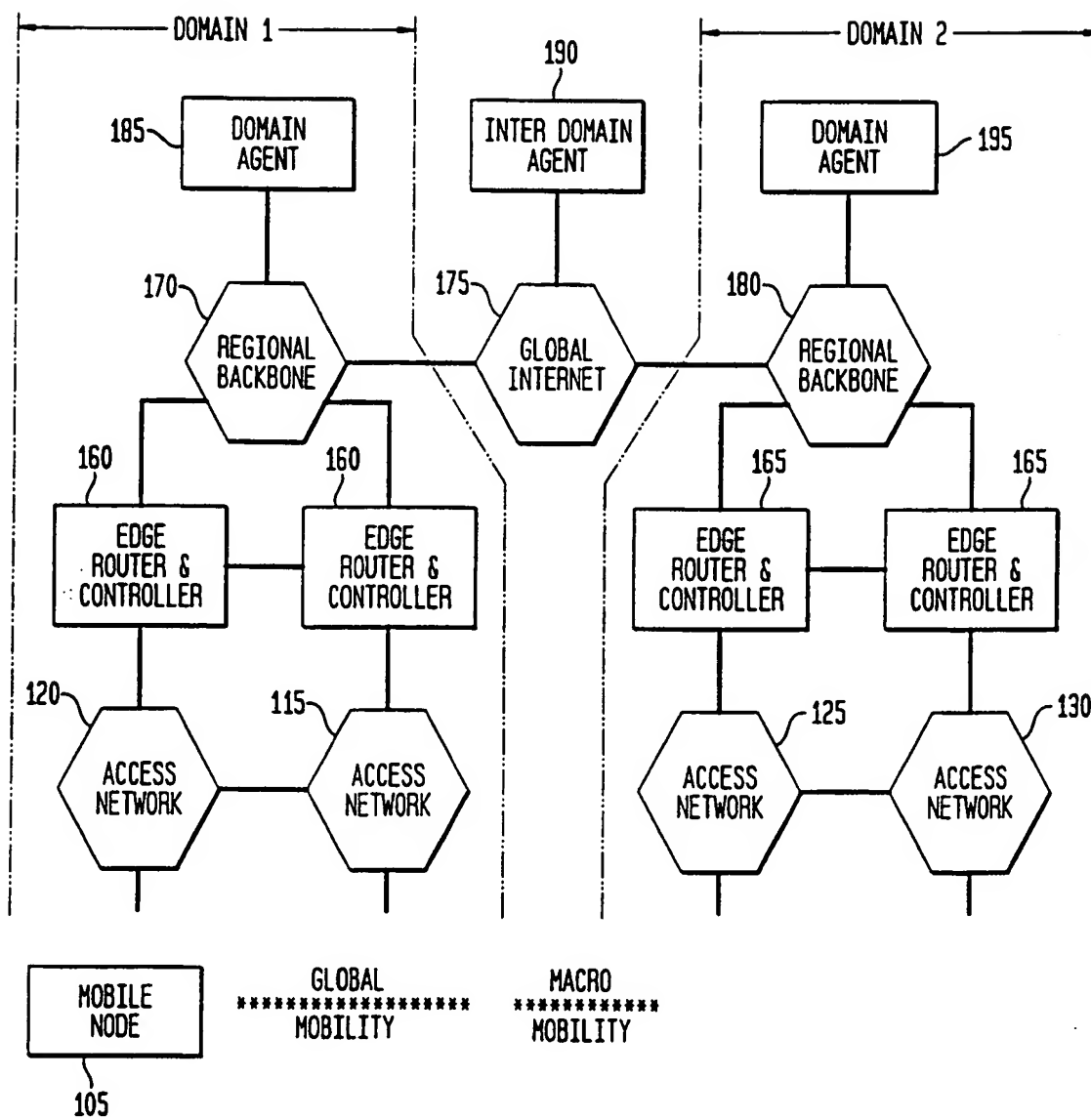
25

16. In an IP based network, a method for rapidly and dynamically registering and configuring a mobile client in a second network environment; said mobile client having traveled from a first network environment to said second network environment, said method comprising:
- 5 providing at least one mobile client in communication with said IP based network; said mobile client:
- requesting an IP address from a server having a plurality of IP addresses and configuration parameters associated; and
- receiving a valid IP address and said configuration parameters from said server;
- 10 said server having already performed an ARP check of said valid IP address thereby eliminating the need for said mobile client to itself perform an ARP check of said valid IP address.
17. A method as in claim 16 further comprising said mobile client repeatedly
- 15 requesting an IP address from said server until either a predetermined time period has expired, a predetermined number of request transmissions has expired or a server has responded to said requests for an IP address.
18. In an IP based network, an apparatus for rapidly and dynamically registering and
- 20 configuring a mobile client in a second network environment; said mobile client having traveled from a first network environment to said second network environment, said apparatus comprising:
- at least one mobile client having an interface for communicating within said IP based network; said mobile unit programmed to:
- 25 request an IP address from a server having a plurality of IP addresses and

configuration parameters associated therewith; and
receive a valid IP address and said configuration parameters from said server;
said server having already performed an ARP check of said valid IP address
thereby eliminating the need for said mobile client to itself perform an ARP
5 check of said valid IP address.

19. An apparatus as in claim 18 wherein said mobile client is further programmed to
repeatedly request an IP address from said server until either a predetermined time
period has expired, a predetermined number of request transmissions has expired or a
10 server has responded to said requests for an IP address.

FIG. 1



2/4

FIG. 2

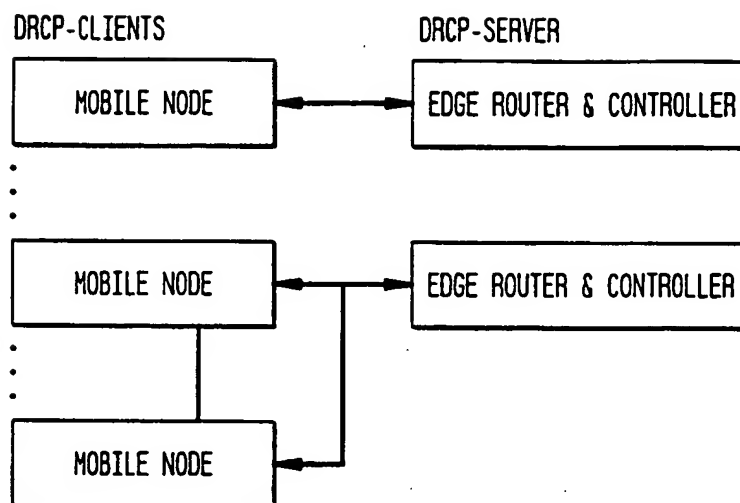


FIG. 3

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------|---|---|---|---|---|---|---|---|---|-----------|---|---|---|---|---|---|---|---|---|----------|---|---|---|---|---|---|---|---|---|---------|---|--|--|--|--|--|--|--|--|
| 0 | | | | | | | | | | 1 | | | | | | | | | | 2 | | | | | | | | | | 3 | | | | | | | | | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | | | | | | | | |
| op (1) | | | | | | | | | | htype (1) | | | | | | | | | | hlen (1) | | | | | | | | | | xid (1) | | | | | | | | | |
| chaddr (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| options (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

3/4

FIG. 4

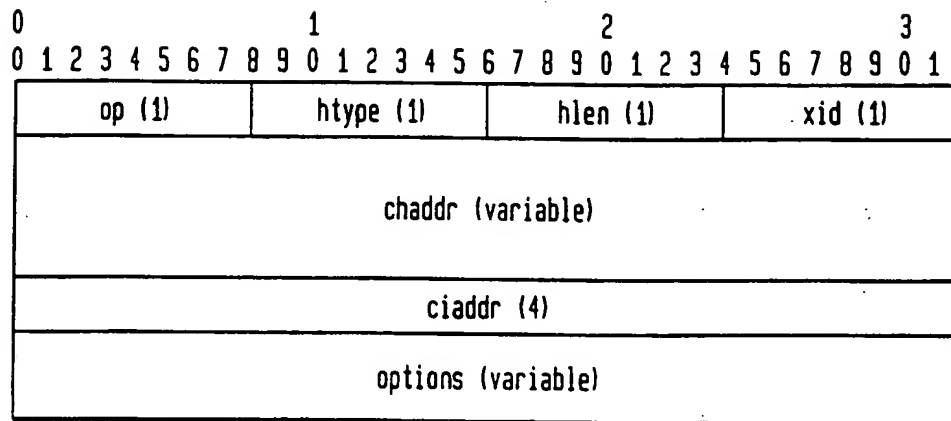


FIG. 5

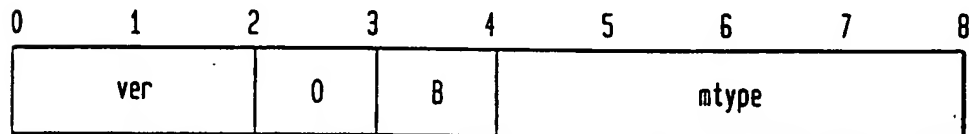
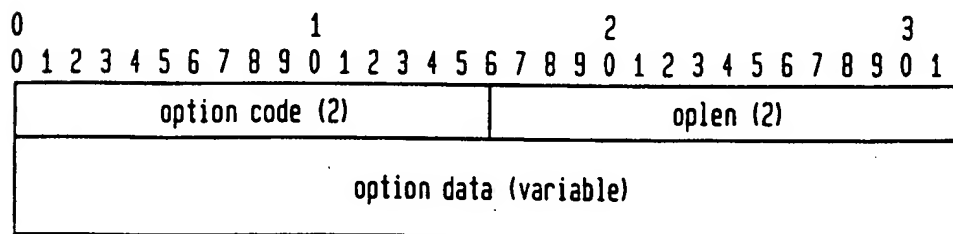


FIG. 6



4/4

FIG. 7

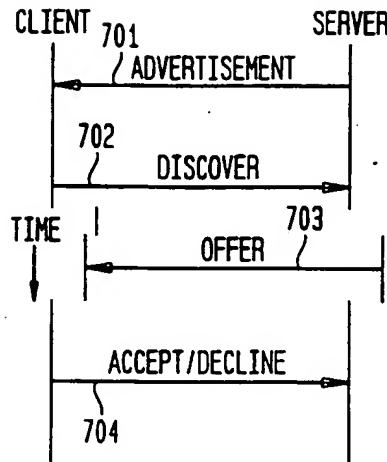


FIG. 8

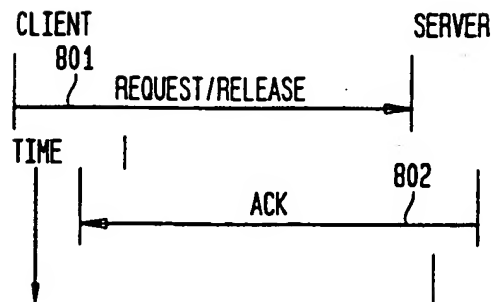
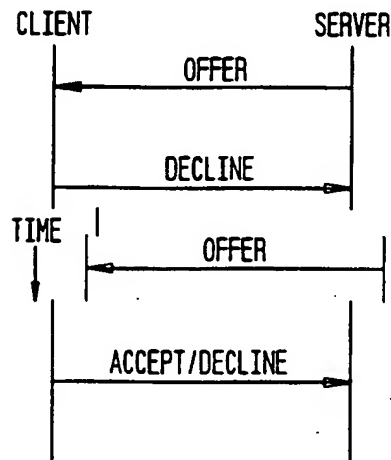


FIG. 9



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/29055

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04J 3/24; H04L 12/46; G06F 15/16

US CL : 370/349, 401; 709/228

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/349, 401; 709/228

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
IEEE publicationsElectronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST, STN

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| X | US 5,983,090 A (AOKI) 09 November 1999, col. 5-9 | 1-19 |
| X | US 5,918,016 (BREWER et al.) 29 June 1999, col. 5-15 | 1-19 |
| X | US 5,159,592 A (PERKINS) 27 OCTOBER 1992, col. 4-9 | 1-19 |
| X | US 5,442,633 A (PERKINS et al.) 15 August 1995, col. 4-11 | 1-19 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | |
|---|--|
| * Special categories of cited documents: | *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| *A* document defining the general state of the art which is not considered to be of particular relevance | *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| *E* earlier document published on or after the international filing date | *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | *A* document member of the same patent family |
| *O* document referring to an oral disclosure, use, exhibition or other means | |
| *P* document published prior to the international filing date but later than the priority date claimed | |

Date of the actual completion of the international search
03 DECEMBER 2000

Date of mailing of the international search report

02 APR 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

SALEH NAJJAR

Telephone No. (703) 308-7613

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.